(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－339227
（P2000－339227A）
(43)公開日　平成12年12月８日(2000.12.8)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ	５Ｂ０１７
Ｇ０６Ｔ　1/00		Ｈ０４Ｎ　1/387		５Ｂ０５７
Ｈ０４Ｎ　1/387		Ｇ０６Ｆ　15/66	Ｂ	５Ｃ０７６

審査請求　未請求　請求項の数17　ＯＬ　（全　９　頁）

(21)出願番号　特願平11－147769

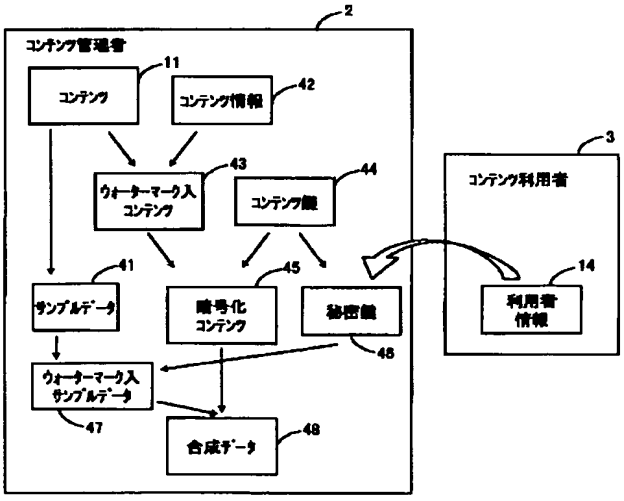
(22)出願日　平成11年５月27日(1999.5.27)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　平野　秀幸
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　小谷　誠剛
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100094145
弁理士　小野　由己男　（外２名）

最終頁に続く

(54)【発明の名称】　データ運用方法

(57)【要約】
【課題】　デジタルコンテンツを暗号化して配布することで著作権の侵害を防止し、かつ暗号化されたデジタルコンテンツを復号化するための許諾情報が破壊されたり、紛失したりすることを防止するデータ運用方法を提供する。
【解決手段】　デジタルコンテンツ１１をコンテンツ鍵４４によって暗号化して暗号化コンテンツ４５を作成し、デジタルコンテンツ１１の一部をサンプルデータ４１として抽出し、コンテンツ鍵４４を利用者情報１４によって暗号化した秘密鍵４６をサンプルデータ４１に不可視情報として埋め込んだウォーターマーク入サンプルデータ４７を作成し、これに暗号化コンテンツ４５を合成した合成データ４８を配布する。



1

【特許請求の範囲】

【請求項１】配布を行うデジタルコンテンツを暗号化して実データ部を作成し、

前記デジタルコンテンツの一部をサンプルデータとして抽出し、前記サンプルデータに前記デジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を不可視情報として埋め込んだサンプルデータ部を作成し、

前記実データ部と前記サンプルデータ部とを合成した合成データを作成してこれを配布するデータ運用方法。

【請求項２】前記サンプルデータ部から許諾情報を分離し、前記許諾情報から前記実データ部を復号化するためのコンテンツ鍵を復元し、このコンテンツ鍵を用いて前記実データ部を元のデジタルコンテンツに復号化して利用することを可能とした、請求項１に記載のデータ運用方法。

【請求項３】前記サンプルデータは、前記デジタルコンテンツ中に含まれる画像データに画像処理、リサイズ、圧縮またはγ補正のうち少なくとも１つの処理を施した画像データである、請求項１または２に記載のデータ運用方法。

【請求項４】前記サンプルデータは、前記実データ部を代表する見出しデータである、請求項１～３のいずれかに記載のデータ運用方法。

【請求項５】前記合成データは、複数のデジタルコンテンツに基づく複数の実データ部と、前記複数の実データ部に対応する複数のサンプルデータ部とを含み、前記複数のサンプルデータ部を構成する各サンプルデータはそれぞれ前記複数の実データ部の対応するものとリンクしている、請求項４に記載のデータ運用方法。

【請求項６】前記サンプルデータ部はＪＰＥＧやＭＰＥＧなどの構造化データであり、前記サンプルデータ部のフォーマットを利用して、前記サンプルデータ部に前記実データ部を追加合成することによって前記合成データを作成する、請求項１～５のいずれかに記載のデータ運用方法。

【請求項７】前記許諾情報は、ユーザ識別情報、ユーザ使用のコンピュータに搭載された機器の識別情報、ユーザ使用のコンピュータに搭載されたＣＰＵの識別情報または前記デジタルコンテンツを格納する記録媒体に固有の識別情報のうちから少なくとも１つを暗号鍵として、前記コンテンツ鍵を暗号化したものである、請求項１～６のいずれかに記載のデータ運用方法。

【請求項８】前記許諾情報は、複数のユーザに共通な識別情報を暗号鍵として、前記コンテンツ鍵を暗号化したものである、請求項１～６のいずれかに記載のデータ運用方法。

【請求項９】前記許諾情報は、前記デジタルコンテンツの配布者固有の識別情報または前記デジタルコンテンツの著作者固有の識別情報のうち少なくとも１つを暗号鍵として、前記コンテンツ鍵を暗号化したものである、請求項１～６のいずれかに記載のデータ運用方法。

2

【請求項１０】前記暗号化されたコンテンツ鍵を復号化するための復号鍵は、暗号化を行う暗号鍵と共通であり、ユーザとコンテンツの配布者間で送受信する一意な情報に基づく共通鍵である、請求項７～９のいずれかに記載のデータ運用方法。

【請求項１１】前記デジタルコンテンツの配布者は、秘密鍵を用いて前記コンテンツ鍵を暗号化し、ユーザは前記デジタルコンテンツの配布者から予め提供されている公開鍵を用いて前記暗号化されたコンテンツ鍵を復号化する、請求項７～９のいずれかに記載のデータ運用方法。

【請求項１２】前記サンプルデータ部は、ユーザが前記デジタルコンテンツを利用した利用回数を不可視情報として備え、ユーザが前記デジタルコンテンツを利用する毎に前記不可視情報を書き換えることを特徴とする、請求項１～１１のいずれかに記載のデータ運用方法。

【請求項１３】前記サンプルデータ部は、利用回数制御を可能とする許諾情報を不可視情報として備え、ユーザが前記デジタルコンテンツを所定回数以上利用した際に、前記不可視情報を書き換えることを特徴とする、請求項１～１１のいずれかに記載のデータ運用方法。

【請求項１４】前記実データ部を復号化して読み込む際またはデジタルコンテンツ利用終了時に、前記不可視情報を書き換えることを特徴とする、請求項１２または１３に記載のデータ運用方法。

【請求項１５】前記サンプルデータ部の不可視情報は、冗長情報を含むことによりエラー回復機能を備える、請求項１２～１４のいずれかに記載のデータ運用方法。

【請求項１６】前記実データ部を復号化する際に、前記サンプルデータ部の不可視情報に基づいて再生する範囲を規制することを特徴とする、請求項１２または１３に記載のデータ運用方法。

【請求項１７】前記実データ部を復号化する際に、前記サンプルデータ部の不可視情報に基づいて再生できる年、月、日、時間のいずれかの範囲を規制することを可能とする、請求項１２または１３に記載のデータ運用方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データ運用方法に関し、特に、デジタルコンテンツを特定の許諾情報で暗号化して配布する際のデータ運用方法に関する。

【０００２】

【従来の技術】コンピュータプログラムなどのソフトウェアや電子出版物では、光磁気ディスク（ＭＯ）、ディジタルビデオディスク（ＤＶＤ）、フロッピーディスク（ＦＤ）、ミニディスク（ＭＤ）、その他の記録媒体上に電子化データを格納して販売される。このような電子

化データは、一般にコピーが容易であり、不正コピーが頻繁に行われている。このため、ソフトウェアベンダーや出版者側の著作権が侵害され著しく利益が阻害されるおそれがある。

【０００３】また、インターネットやＣＡＴＶ、その他のネットワークなどを通じて配布される静止画像データ、動画像データを含む電子化データについても同様にして不正コピーが頻繁に行われ、著作権者の利益が損なわれている。このような記録媒体上に格納された電子化データや各種ネットワークを通じて配布される電子化データなどのいわゆるデジタルコンテンツを保護するために、暗号鍵を用いてデジタルコンテンツを暗号化しこの暗号化された実データを配布することが行われる。

【０００４】たとえば、ユーザが自分のパーソナルコンピュータからコンテンツの配布者側にアクセスを行い、デジタルコンテンツをハードディスク上にダウンロードを行ってこれを利用する場合を考える。まず、ユーザはホストコンピュータにアクセスしてダウンロードのためのプラグインモジュールを入手する。この後、使用しているハードディスクドライブの識別番号、使用しているコンピュータのＣＰＵ識別番号、その他ユーザ固有の識別情報をホストコンピュータ側に送付する。

【０００５】コンテンツの配布者側では、デジタルコンテンツをコンテンツ鍵で暗号化した実データと、コンテンツ鍵をユーザ固有の識別情報で暗号化した許諾情報を、ユーザ側に送信する。ユーザ側では、送られてきた暗号化実データと、許諾情報とを暗号化された状態のままハードディスクに記録する。デジタルコンテンツを利用する場合には、ハードディスクドライブの識別番号などのユーザ固有の識別情報を用いて、許諾情報を復号化し、コンテンツ鍵を取得する。このコンテンツ鍵を用いて、暗号化されたデジタルコンテンツを復号化してこれを利用する。

【０００６】この場合、ユーザ個々にデジタルコンテンツの利用権を与える際に、デジタルコンテンツを暗号化するための暗号鍵を共通にすることができ、ユーザ毎に異なるユーザ固有の情報を用いて復号鍵を暗号化することによって、利用権を個々に与えることが可能となる。

【０００７】

【発明が解決しようとする課題】上述の方法でデータの配布を行う場合、データ配布者は暗号化されたデジタルコンテンツと、暗号化されたデジタルコンテンツの復号鍵となる許諾情報とを別々に送付する必要がある。また、ユーザ側においても、送付されてくる暗号化されたデジタルコンテンツとその許諾情報とを別々に記録媒体に格納しておく必要がある。

【０００８】したがって、データ配布者側からユーザ側に送付される途中で許諾情報が破壊されたり、またはユーザ側の記録媒体上で許諾情報がなんらかの事故により破壊もしくは紛失した場合には、デジタルコンテンツを利用することができなくなり、再度許諾情報を入手する手順が必要となる。本発明は、デジタルコンテンツを暗号化して配布することで著作権の侵害を防止し、かつ暗号化されたデジタルコンテンツを復号化するための許諾情報が破壊されたり、紛失したりすることを防止するデータ運用方法を提供する。

【０００９】

【課題を解決するための手段】本発明に係るデータ運用方法は、配布を行うデジタルコンテンツを暗号化して実データ部を作成し、デジタルコンテンツの一部をサンプルデータとして抽出し、サンプルデータにデジタルコンテンツを暗号化する際の暗号鍵として用いたコンテンツ鍵の情報を含む許諾情報を不可視情報として埋め込んだサンプルデータ部を作成し、実データ部と前記サンプルデータ部とを合成した合成データを作成してこれを配布する。

【００１０】配布されたデジタルコンテンツを利用する場合には、サンプルデータ部から許諾情報を分離し、許諾情報から実データ部を復号化するためのコンテンツ鍵を復元し、このコンテンツ鍵を用いて実データ部を元のデジタルコンテンツに復号化して利用する。このことにより、実データ部とサンプルデータ部に不可視情報として埋め込まれた許諾情報とが一体化されており、実データ部を復号化するための許諾情報が破壊されたり紛失したりすることを防止できるとともに、この一体化されたデータを流通させることによりデータの配布が可能となるため、システムをコンパクトにすることができる。

【００１１】サンプルデータは、デジタルコンテンツ中に含まれる画像データに画像処理、リサイズ、圧縮またはγ補正のうち少なくとも１つの処理を施した画像データとすることができる。また、サンプルデータは実データ部を代表する見出しデータとすることができる。

【００１２】さらに、合成データは、複数のデジタルコンテンツに基づく複数の実データ部と、複数の実データ部に対応する複数のサンプルデータ部とを含み、複数のサンプルデータ部を構成する各サンプルデータはそれぞれ複数の実データ部の対応するものとリンクするように構成できる。また、サンプルデータ部はＪＰＥＧやＭＰＥＧなどの構造化データであり、サンプルデータ部のフォーマットを利用して、サンプルデータ部に実データ部を追加合成することによって合成データを作成するように構成できる。

【００１３】許諾情報は、ユーザ識別情報、ユーザ使用のコンピュータに搭載された機器の識別情報、ユーザ使用のコンピュータに搭載されたＣＰＵの識別情報またはデジタルコンテンツを格納する記録媒体に固有の識別情報のうちから少なくとも１つを暗号鍵として、コンテンツ鍵を暗号化したものとすることができ、複数のユーザに共通な識別情報を暗号鍵として、コンテンツ鍵を暗号化したものとすることも可能であり、さらに、デジタル

コンテンツの配布者固有の識別情報またはデジタルコンテンツの著作者固有の識別情報のうち少なくとも１つを暗号鍵として、コンテンツ鍵を暗号化したものとすることもできる。

【００１４】暗号化されたコンテンツ鍵を復号化するための復号鍵は、暗号化を行う暗号鍵と共通であり、ユーザとコンテンツの配布者間で送受信する一意な情報に基づく共通鍵とすることができる。また、デジタルコンテンツの配布者は、秘密鍵を用いてコンテンツ鍵を暗号化し、ユーザはデジタルコンテンツの配布者から予め提供されている公開鍵を用いて暗号化されたコンテンツ鍵を復号化するように構成することも可能である。

【００１５】また、サンプルデータ部は、ユーザがデジタルコンテンツを利用した利用回数を不可視情報として備え、ユーザがデジタルコンテンツを利用する毎に不可視情報を書き換えるように構成できる。さらに、サンプルデータ部は、利用回数制御を許諾情報を不可視情報として備え、ユーザがデジタルコンテンツを所定回数以上利用した際に、不可視情報を書き換えるように構成できる。

【００１６】この場合、実データ部を復号化して読み込む際またはデジタルコンテンツ利用終了時に、不可視情報を書き換えるように構成できる。また、サンプルデータ部の不可視情報は、冗長情報を含むことによりエラー回復機能を備える構成とすることができる。実データ部を復号化する際に、サンプルデータ部の不可視情報に基づいて再生する範囲を規制するように構成でき、実データ部を復号化する際に、サンプルデータ部の不可視情報に基づいて再生できる年、月、日、時間のいずれかの範囲を規制するように構成できる。

【００１７】

【発明の実施の形態】〔発明の概要〕図１に本発明の概要構成を示す。コンテンツ提供者１は、デジタルコンテンツの著作者、版権者などであり、運用を行うデジタルコンテンツ１１をコンテンツ管理者２に提供する。

【００１８】コンテンツ管理者２は、コンテンツ提供者１から提供されるデジタルコンテンツ１１を運用するために暗号化し、この暗号鍵を管理するとともに、このデジタルコンテンツ１１を利用するユーザの利用者情報を管理する。コンテンツ利用者３は、コンテンツ管理者２が管理しているデジタルコンテンツを利用したい場合には、利用者情報１４をコンテンツ管理者２に送信する。

【００１９】コンテンツ管理者２は、コンテンツ利用者３から送信された利用者情報１４を管理するとともに、この利用者情報１４に基づくコンテンツ使用許諾情報１３を作成し、暗号化コンテンツ１２と一体化してコンテンツ利用者３に送信する。このとき、コンテンツ管理者２はデジタルコンテンツ１１からコンテンツの内容を代表するようなサンプルデータを抽出する。デジタルコンテンツ１１を暗号化した暗号鍵を利用者情報１４によって暗号化してコンテンツ使用許諾情報１３を作成し、これをサンプルデータ中に不可視情報として埋込んだサンプルデータ部を作成する。さらに、このサンプルデータ部を暗号化コンテンツ１２と合成してコンテンツ利用者３に送信する。このとき、コンテンツ提供者１とコンテンツ管理者２は同一であってもよい。

【００２０】〔コンテンツ管理者〕コンテンツ管理者２側の概略構成を示す機能ブロック図を図２に示す。このコンテンツ管理者２側では、運用を行うコンテンツを管理するコンテンツ管理部２１、所定のコンテンツ鍵を用いてデジタルコンテンツを暗号化するコンテンツ暗号化部２２、コンテンツ鍵を管理するコンテンツ鍵管理部２３、コンテンツ利用者３の利用者情報を取得してこれを管理する利用者情報管理部２４、利用者情報管理部２４で管理している利用者情報情報に基づいてデジタルコンテンツの利用許諾情報を作成しこれを管理する許諾情報管理部２５、デジタルコンテンツからサンプルデータを抽出しこれに許諾情報を不可視情報として埋め込む許諾情報入サンプル作成部２６、コンテンツ鍵を用いて暗号化した暗号化コンテンツと許諾情報入サンプルデータとを合成する暗号化コンテンツ合成部２７などを備えている。

【００２１】〔コンテンツ利用者〕コンテンツ利用者３側の概略構成を示す機能ブロック図を図３に示す。このコンテンツ利用者３側では、使用しているハードディスクドライブの識別番号、コンピュータに搭載されているＣＰＵの識別番号、その他の利用者固有の識別情報を管理する利用者情報管理部３１、コンテンツ管理者２からの合成データを取得するための合成データ取得部３２、取得した合成データのうちサンプルデータを表示するためのサンプルデータ表示部３３、許諾情報入サンプルデータから許諾情報を分離する許諾情報抽出部３４、抽出した許諾情報を復号化してコンテンツ鍵を再生するコンテンツ鍵復号部３５、復号化されたコンテンツ鍵を用いて暗号化コンテンツを復号化するコンテンツ復号部３６、復号化したデジタルコンテンツを動作させるコンテンツ動作部３７などを備えている。

【００２２】〔コンテンツ配布〕デジタルコンテンツを配布する際にコンテンツ管理者２側が行う動作を図４、図５に基づいて説明する。デジタルコンテンツ１１は、そのコンテンツ情報４２が電子透かし（ウォーターマーク）として埋め込まれてウォーターマーク入コンテンツ４３となる。ここでは、データの特定の周波数帯域にコンテンツ情報４２を挿入するように構成でき、またデータの一部を間引きし、ここにコンテンツ情報４２を挿入するように構成することもできる。コンテンツ情報４２は、たとえばこのデジタルコンテンツ１１の著作権情報とすることができ、このような情報の埋込を省略することも可能である。

【００２３】ステップＳ１では、コンテンツ鍵４４を用

いてウォーターマーク入コンテンツ４３を暗号化し、暗号化コンテンツ４５を作成する。ステップＳ２では、利用者情報１４を獲得する。ここでは、コンテンツ利用者２側からアクセスがあった場合に、コンテンツ利用者２が使用しているハードディスクドライブの識別番号、コンピュータに搭載されているＣＰＵの識別番号などのコンテンツ利用者３に固有の識別情報を送信させ、これを利用者情報管理部２４（図２参照）に格納しておく。

【００２４】ステップＳ３では、獲得した利用者情報１４を用いてコンテンツ鍵４４を暗号化し、秘密鍵４６を作成する。この秘密鍵４６は、コンテンツ利用者３に固有の利用者情報１４に基づいて暗号化されているため、このデジタルコンテンツ１１を利用するための許諾情報となっている。ステップＳ４では、デジタルコンテンツ１１からこのコンテンツを代表するようなデータをサンプルデータ４１として抽出する。デジタルコンテンツ１１が複数の画像データを含む場合、このうちの１つの画像データをサンプルデータ４１として抽出することができる。複数のデジタルコンテンツ１１を同時に運用する場合には、ここで抽出したサンプルデータ４１を対応するデジタルコンテンツ１１とリンクさせ、複数のサンプルデータのうちから所望のものを選択させ、利用するデジタルコンテンツを選ぶことができるように構成できる。

【００２５】ステップＳ５では、サンプルデータ４１に秘密鍵４６を電子透かしとして埋め込んでウォーターマーク入サンプルデータ４７を作成する。このウォーターマーク入サンプルデータ４７は、前述と同様に、データの特定の周波数帯域に秘密鍵４６のデータを挿入するように構成でき、またデータの一部を間引きし、ここに秘密鍵４６のデータを挿入するように構成することもできる。このことにより、許諾情報が不可視情報として埋め込まれた許諾情報入サンプルデータが作成されたこととなる。

【００２６】ステップＳ６では、暗号化コンテンツ４５とウォーターマーク入サンプルデータ４７とを合成して合成データ４８を作成する。デジタルコンテンツ１１が複数の画像データよりなる場合には、サンプルデータをJPEGなどの構造化データ形式にしてデータを配布することができる。この場合、サンプルデータ４１とデジタルコンテンツ１１をペアとし、コンテンツ毎に許諾情報を埋め込んでウォーターマーク入りサンプルデータ４７作成し、デジタルコンテンツ１１をサンプルデータ４７に追加合成する。

【００２７】このときのJPEGデータ構造を図８に示す。ウォーターマーク入サンプルデータ４７は、イメージデータの始点(SOI) ６３、イメージデータの終点（EOI）６５および始点６３と終点６５に挟まれるフレーム６４とからなるサンプルデータ部６１として構成されている。また、コンテンツ鍵４４で暗号化されたデジタルコンテンツ６６が実データ部６２を構成し、このサンプルデータ部６１および実データ部６２が一体的に合成されている。

【００２８】ステップＳ７では、コンテンツ利用者３の要望に応じて合成データ４８を送信する。各種ネットワークなどを通じて配信する場合には、合成データ４８をそのネットワークを通じて送信することとなるが、CD-ROM、ＤＶＤ、その他の記録媒体に記録してこれを配布することも可能である。

【００２９】〔コンテンツ利用〕コンテンツ利用者３が配布されたデジタルコンテンツを利用する場合の動作を図６、図７に基づいて説明する。ステップＳ２１では、コンテンツ管理者２から合成データ４８を取得する。このとき、コンテンツ利用者３は、予めコンテンツ管理者２側にアクセスを行い、コンテンツ管理者２が管理しているデジタルコンテンツを利用した旨を伝え、利用者固有の利用者情報１４をコンテンツ管理者２側に送っているものとする。合成データ４８は、各種ネットワークを通じてデータをダウンロードして得る形態であってもよく、またコンテンツ管理者２から記録媒体に記録された状態で配布されることによって得るような形態であってもよい。取得した合成データ４８は、コンテンツ利用者３が使用しているハードディスク、その他の記録媒体上に格納される。

【００３０】ステップＳ２２では、合成データ４８のうちからウォーターマーク入サンプルデータ５０を表示させる。合成データ４８内に複数のデジタルコンテンツを含む場合には、各デジタルコンテンツに対応するウォーターマーク入サンプルデータ４７を縮小して並べたり、スクロールや切替などで順次表示させることでカタログ表示機能を持たせることが可能であり、クライアントソフト側でこのような機能を持たせることができる。合成データ４８内に１つのデジタルコンテンツしか存在しない場合であっても、いくつかのサンプルデータを抽出してサンプルデータ部を構成し、これをカタログ表示させるように構成することも可能である。もちろん、サンプルデータがひとつの場合にはこれをそのまま表示するように構成できる。ステップＳ２３では、コンテンツ利用者３による利用要求があったか否かを判別する。ウォーターマーク入サンプルデータ５０の表示において、コンテンツ利用者３が特定のサンプルデータを選択してこれを利用する旨の指示を行った場合には、ステップＳ２４に移行してコンテンツ利用ソフトを動作させる。

【００３１】ステップＳ２４では、合成データ４８のウォーターマーク入サンプルデータ４７から許諾情報を分離する。ここでは、ウォーターマーク入サンプルデータ４７にウォーターマークとして埋め込まれている秘密鍵４６を取り出す。秘密鍵４６がサンプルデータの周波数成分として埋め込まれている場合には、ウォーターマーク入サンプルデータ４７を周波数解析することにより秘

密鍵４６を取り出すことができる。また、サンプルデータを間引きしてウォーターマークを埋め込んだ場合などの物理的埋込みが行われている場合には、画像解析を行って秘密鍵４６を取り出すことが可能となる。

【００３２】ステップＳ２５では、取り出した秘密鍵４６を利用者情報１４を用いて復号化し、コンテンツ鍵４４を再生する。ステップＳ２６では再生したコンテンツ鍵４４を用いて暗号化コンテンツ４５を復号化し、ウォーターマーク入コンテンツ４３をハードディスク上に展開する。ステップＳ２７では、実際にウォーターマーク入コンテンツ４３を動作させてコンテンツ利用を実行する。

【００３３】〔データ運用の形態〕図９に示すような運用形態をとることも可能である。コンテンツ提供者５１は、デジタルコンテンツの著作者、版権を有する版元などであり、コンテンツ管理者５２にデジタルコンテンツを提供する(A)。

【００３４】コンテンツ管理者５２は、コンテンツ提供者５１から提供されたデジタルコンテンツをコンテンツ鍵を用いて暗号化する。コンテンツ管理者５２は、暗号化されたデジタルコンテンツおよびコンテンツ鍵をデータの実際の配布を行うセンター５３に送信する(B)。センター５３は、暗号化されたデジタルコンテンツおよびコンテンツ鍵を管理する。このセンター５３は、インターネット、その他各種ネットワーク内のＷＥＢサーバであり、ユーザ５４からのアクセスに対応して、デジタルコンテンツの配布を行うように構成される。

【００３５】ユーザ５４は、ＷＥＢブラウザに利用してセンター５３にアクセスし、データ取得のためのプラグインモジュールを取得する(C)。ユーザ５４は、ＷＥＢブラウザ上でプラグインモジュールを起動し、自己の使用しているハードディスクドライブの識別番号などのユーザ固有の識別情報をセンター５３に送出する(D)。センター５３では、ユーザ固有の識別情報に基づいてコンテンツ鍵を暗号化して許諾情報を作成し、デジタルコンテンツのサンプルデータにウォーターマークとして埋め込み、暗号化コンテンツと合成して許諾情報入暗号化コンテンツを作成する。この許諾情報入暗号化コンテンツをコンテンツ利用者５４に送信する(E)。

【００３６】コンテンツ利用者５４側では、受け取った許諾情報入暗号化コンテンツをハードディスクなどの利用者ディスク５５に格納する (F)。デジタルコンテンツを利用する場合には、利用者ディスク５５に格納されている許諾情報入暗号化コンテンツから、ユーザ固有の識別情報を用いてコンテンツ鍵を取り出し(G)、暗号化コンテンツをコンテンツ鍵で復号化してデジタルコンテンツを取り出す(H)。

【００３７】このように、構成するこにより、デジタルコンテンツを暗号化するためのコンテンツ鍵をコンテンツ利用者毎に変える必要がなく、１つのデジタルコンテンツについて１つのコンテンツ鍵とすることができ、暗号鍵の管理が容易となる。また、コンテンツ利用者固有の識別情報により許諾情報のセキュリティが守られており、デジタルコンテンツの不正利用を防止することが可能となる。さらに、許諾情報が暗号化コンテンツと一体化されているため、鍵の受け渡しの手順が簡単になるとともに、暗号化コンテンツを復号化するための鍵を紛失したり破壊されたりすることがなく、鍵の再発行などの手間を省くことができる。

【００３８】〔他の実施形態〕

（Ａ）コンテンツ利用者２側で、取得した合成データを格納し、これを復号化して展開する記録媒体は、ハードディスクの他に、ＭＯ、ＺＩＰ、ＤＶＤ、ＩＣメモリ、その他のものが可能であり、その場合、利用者情報１４としてこれらの装置ＩＤを用いることができる。

【００３９】（Ｂ）また、デジタルコンテンツが、ＣＤ－ＲＯＭやＤＶＤなどの記録媒体に記録されて配布される形態の場合、パッケージ内に記載されているコンテンツＩＤや媒体識別番号などを利用者情報１４とすることもできる。

（Ｃ）ウォーターマーク入サンプルデータ４７内に埋め込まれた許諾情報には、コンテンツ利用者２がデジタルコンテンツを復号化して利用した回数を記録する領域を含むように構成できる。この場合、予め設定した回数を超えて利用しようとした場合に、これを規制するように構成することが可能である。利用した回数は、暗号化コンテンツを読み込んで復号化する際またはデジタルコンテンツの利用終了時に、利用回数を更新し、これを不可視情報としてウォーターマーク入サンプルデータ４７を書き換えるように構成できる。

【００４０】（Ｄ）ウォーターマーク入サンプルデータ４７内に埋め込まれた許諾情報には、利用者情報１４を記録する領域を含むように構成できる。この場合、デジタルコンテンツの不正コピーや不正な流通を防止できる。

（Ｅ）ウォーターマーク入サンプルデータ４７内に埋め込まれた許諾情報は、複数繰り返された冗長情報とすることができる。このことにより、エラー回復機能を持たせることが可能であり、許諾情報に基づく秘密鍵４６の喪失を防止することができる。

【００４１】（Ｆ）ウォーターマーク入りサンプルデータ４７内に埋め込まれた許諾情報は、再生できる年、月、日、時間のいずれかの範囲を規制するように構成することができる。この場合、デジタルコンテンツの不正コピーや不正な流通を防止できる。

（Ｇ）ウォーターマーク入りサンプルデータ４７内に埋め込まれた許諾情報は、利用回数制御を可能とするように構成することができる。この場合、デジタルコンテンツの不正コピーや不正な流通を防止できる。

【００４２】

【発明の効果】本発明によれば、許諾情報を含むサンプルデータ部とデジタルコンテンツを暗号化した実データ部とを一体的に合成した合成データとしてこれを配布しているため、実データ部を復号化するための鍵を実データ部と別にやりとりする必要がなく、また、ユーザ側においても実データ部と鍵とを別に管理する必要がないため、実データ部を復号化するための鍵を紛失することがなく、再発行などの煩雑な処理がなくなる。

【００４３】許諾情報は、サンプルデータに不可視情報として埋め込まれているため、セキュリティを高く維持することができる。

【図面の簡単な説明】

【図１】本発明の概略構成図。

【図２】コンテンツ管理者側の概略構成図。

【図３】コンテンツ利用者側の概略構成図。

【図４】コンテンツ配布時の原理図。

【図５】コンテンツ配布時のフローチャート。

【図６】コンテンツ利用時の原理図。

【図７】コンテンツ利用時のフローチャート。

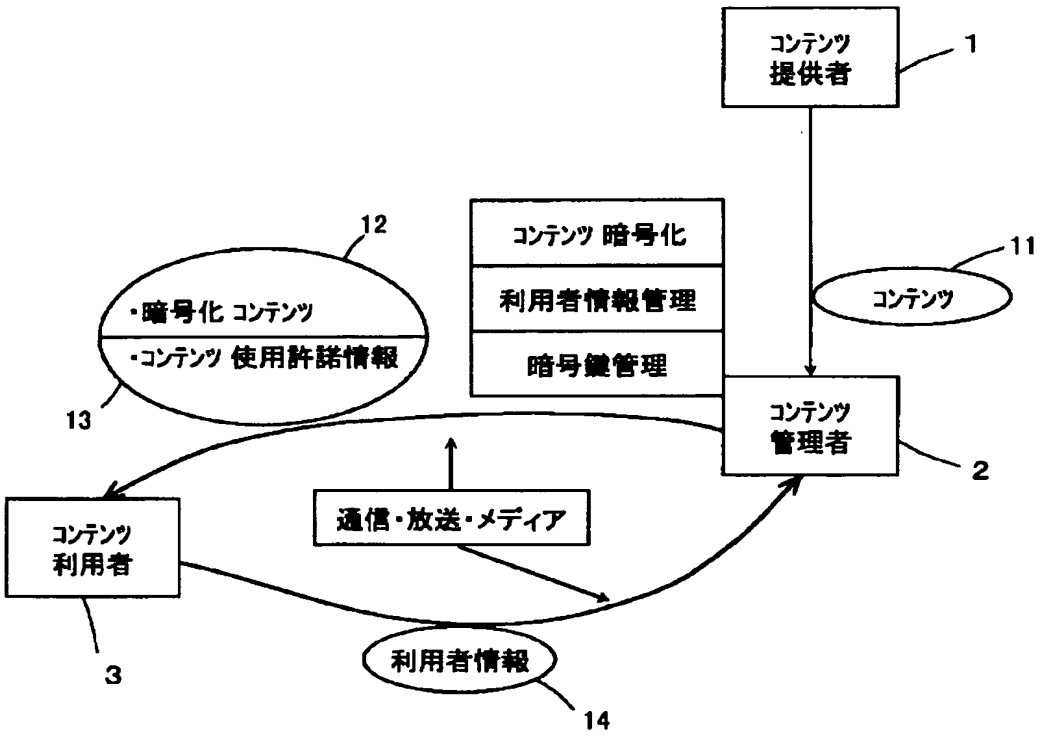
【図８】JPEGデータの構造を示す説明図。

【図９】運用形態の１例を示す構成図。

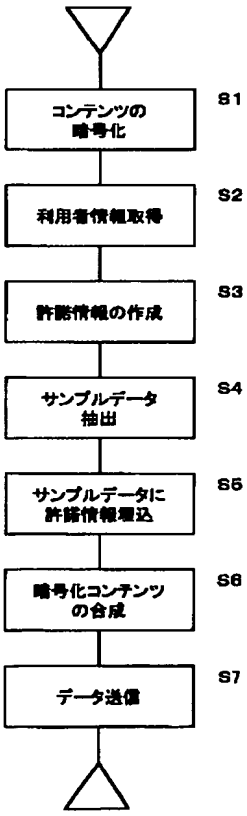
【符号の説明】

１　コンテンツ提供者
２　コンテンツ管理者
３　コンテンツ利用者
１１　デジタルコンテンツ
１２　暗号化コンテンツ
１３　コンテンツ使用許諾情報
１４　利用者情報
４１　サンプルデータ
４２　ウォーターマーク入サンプルデータ
４３　ウォーターマーク入コンテンツ
４４　コンテンツ鍵
４５　暗号化コンテンツ
４６　秘密鍵
４７　ウォーターマーク入サンプルデータ
４８　合成データ

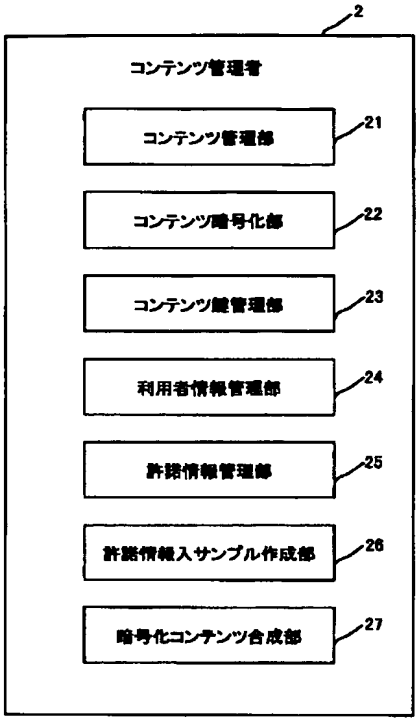
【図１】



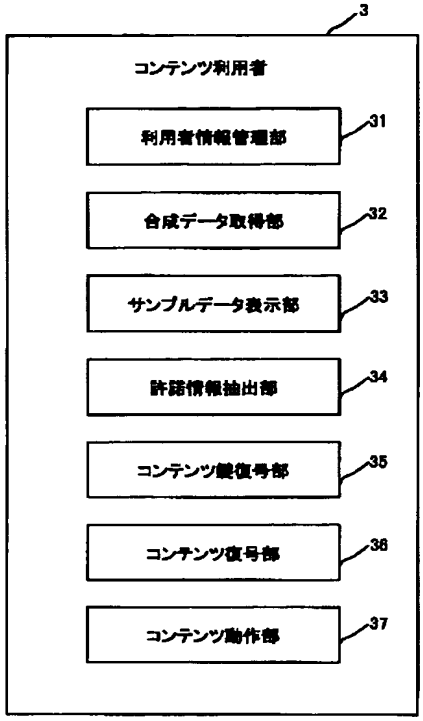
【図５】



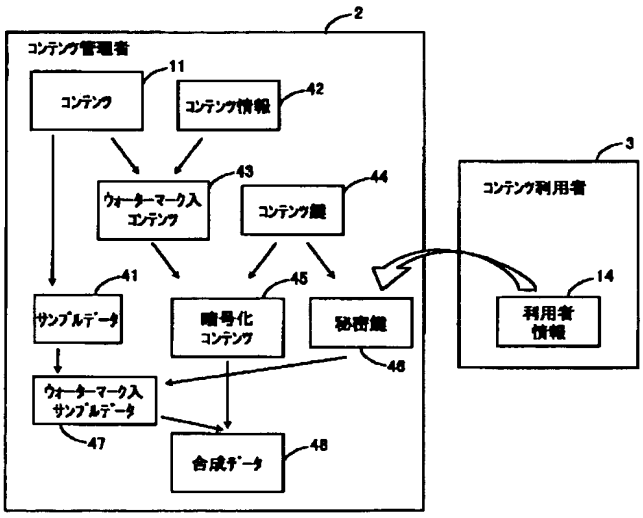
【図２】


2
コンテンツ管理者
コンテンツ管理部
21
コンテンツ暗号化部
22
コンテンツ鍵管理部
23
利用者情報管理部
24
許諾情報管理部
25
許諾情報入サンプル作成部
26
暗号化コンテンツ合成部
27

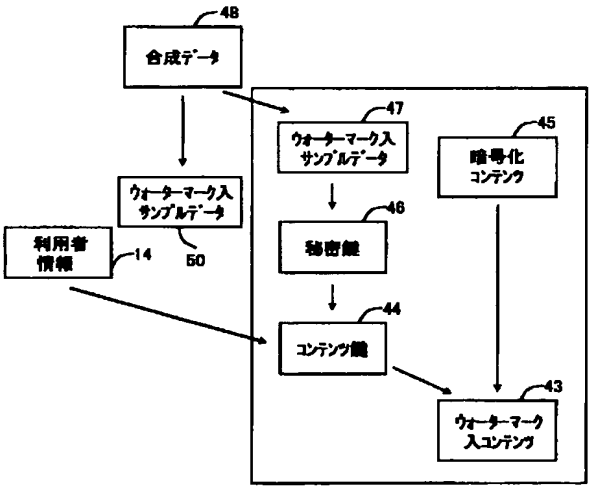
【図３】


3
コンテンツ利用者
利用者情報管理部
31
合成データ取得部
32
サンプルデータ表示部
33
許諾情報抽出部
34
コンテンツ鍵復号部
35
コンテンツ復号部
36
コンテンツ動作部
37

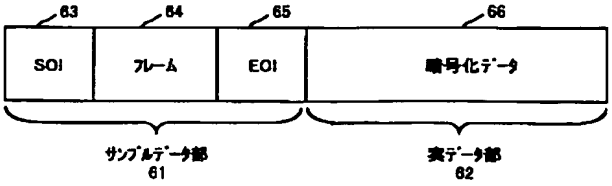
【図４】


2
コンテンツ管理者
コンテンツ
11
コンテンツ情報
42
ウォーターマーク入コンテンツ
43
コンテンツ鍵
44
サンプルデータ
41
暗号化コンテンツ
45
秘密鍵
46
ウォーターマーク入サンプルデータ
47
合成データ
48
3
コンテンツ利用者
利用者情報
14

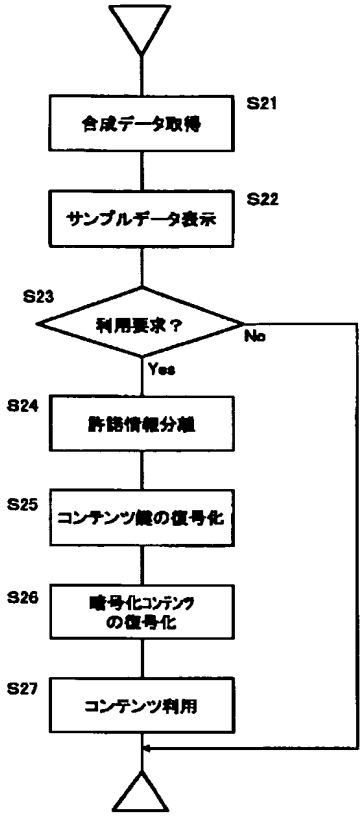
【図６】


48
合成データ
47
ウォーターマーク入サンプルデータ
45
暗号化コンテンツ
ウォーターマーク入サンプルデータ
50
利用者情報
14
46
秘密鍵
44
コンテンツ鍵
43
ウォーターマーク入コンテンツ

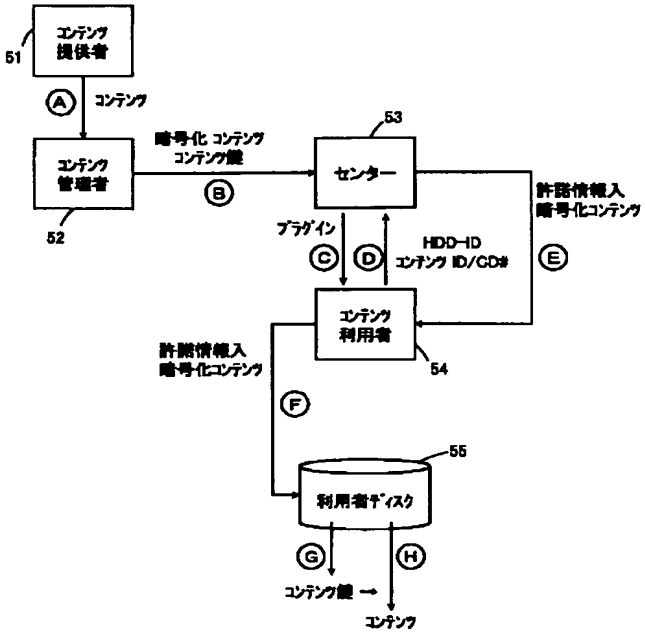
【図８】


63
64
65
66
SOI
フレーム
EOI
暗号化データ
サンプルデータ部
61
実データ部
62

【図７】



【図９】



フロントページの続き

(72)発明者　橋本　晋二
神奈川県川崎市中原区上小田中４丁目１番
１号　富士通株式会社内

Ｆターム(参考)　5B017 AA06 BA07 BB02 CA06 CA09
5B057 CA16 CA18 CB16 CB18 CD05
CE11 CG07
5C076 AA14